IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

FAIRWAY IP LLC, Plaintiff, v. **ULTRA ELECTRONICS ADVANCED TACTICAL SYSTEMS, INC.; and ULTRA ELECTRONICS DEFENSE, INC.** Defendant.	**Civil Action No. 6:20-cv-1024** **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiff Fairway IP LLC ("Fairway") files this original complaint against Ultra Electronics Advanced Tactical Systems, Inc., and Ultra Electronics Defense, Inc, ("collectively Defendants"), alleging, based on its own knowledge as to itself and its own actions, and based on information and belief as to all other matters, as follows:

PARTIES

1. Fairway IP LLC is a limited liability company formed under the laws of the State of Texas.

2. On information and belief, Ultra Electronics Advanced Tactical Systems, Inc., is a Texas Corporation with a principal place of business at 4101 Smith School Rd. Ste., 100, Building IV, Austin, TX 78744.

3. Based upon public information, Defendant Ultra Electronics Defense, Inc. ("Ultra") is a Delaware corporation with a listed registered agent of The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801. Upon information and belief, UEATS is a subsidiary of Ultra.

JURISDICTION AND VENUE

4. This is an action for infringement of a United States patent arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. §§ 1331 and 1338(a).

5. Venue is proper in this District under 28 U.S.C. §§ 1391.

6. Defendant is subject to this Court's specific and general personal jurisdiction under due process and/or the Texas Long Arm Statute due at least to Defendant's substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this district.

7. Furthermore, upon information and belief Defendant maintains subsidiaries in the State of Texas.

THE '405 PATENT

8. On February 27, 2007, United States Patent No. 7,184,405 ("the '405 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention titled "Method for Setting Up a Communication Link in a Telecommunication Network." A true and correct copy has been attached hereto as Exhibit A.

9. The ’405 Patent generally covers “a method for setting up a connection for a communication network having a multiplicity of network nodes networked via links.” ’405 Patent, 1:60-62.

10. The ’405 Patent recognized several problems with existing “connectionless and connection-oriented transmission methods which are used for rapidly transmitting data packets via a communication network.” *Id.* at 1:19-22. Prior art connectionless transmission methods using a “conventional router based on the IP must compare a destination IP address of a received IP data packet with entries in its routing table in order to determine, via a so-called longest match, the link via which the IP data packet is to be forwarded.” *Id.* at 1:30-34. However, a label switching router, in contrast, receives the IP data packet together with a prefixed label and uses this label as table index in order to take from a table the information for identifying the link for forwarding the IP data and a new label is forwarded together with the IP data packet instead of the received label. *Id.* at 1:34-39.

11. To fully exploit this, the ’405 Patent disclosed a method which included “determining routes to destination network nodes of connection destinations for the network nodes, allocating, in the network nodes, an allocation rule by means of the routes determined, by means of which a forwarding information item is allocated both to a link leading in the direction of this destination node and to a new forwarding information item for each destination network node and transmitting a setup message from an originating network node to the destination network nodes for preparing a subsequent transmission of data, such that in a network node receiving the setup message.” *Id.* at 1:63-2:6. The method further included forwarding a information item included in the setup message is read out and using the allocation rule, the setup message is forwarded via a link allocated to this forwarding information items in this network node, after replacement of this

forwarding information item by a new forwarding information item allocated to the former information item. *Id.* at 2:7-13.

12. The inventions of the '405 Patent solved the problems by providing a method for setting up a connection for a communication network which allows rapid transmission of a setup message." *Id.* at 4:23-25. Under the invention, the method allows setup messages to be transmitted by a communication network with approximately the same speed as useful data packets transmitted in a connection which has been set up. *Id.* at 4:26-29.

13. Fairway is the owner of the '405 Patent with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the '405 patent against infringers, and to collect damages for all relevant times.

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 7,184,405

14. Fairway repeats and realleges the allegations of paragraphs 1 through 13 as if fully set forth herein.

15. Defendant, without authority from Fairway, made, had made, used, imported, provided, supplied, distributed, sold, and/or offered for sale access-control systems and other products which practices a method for setting up a connection for a communication network having a multiplicity of network nodes networked via link. When placed into operation by Defendant, these acts constitute direct infringement (literally and/or under the doctrine of equivalents) under 35 U.S.C. § 271(a). To the extent Defendant had knowledge of the '405 Patent, when placed into operation by Defendant's end users, these acts constitute direct infringement by the end users and inducement by Defendant.

16. The Accused Products include at least the following models and/or systems: AirGuard WiMesh End Point 3e-523N, and all other substantially similar products (collectively

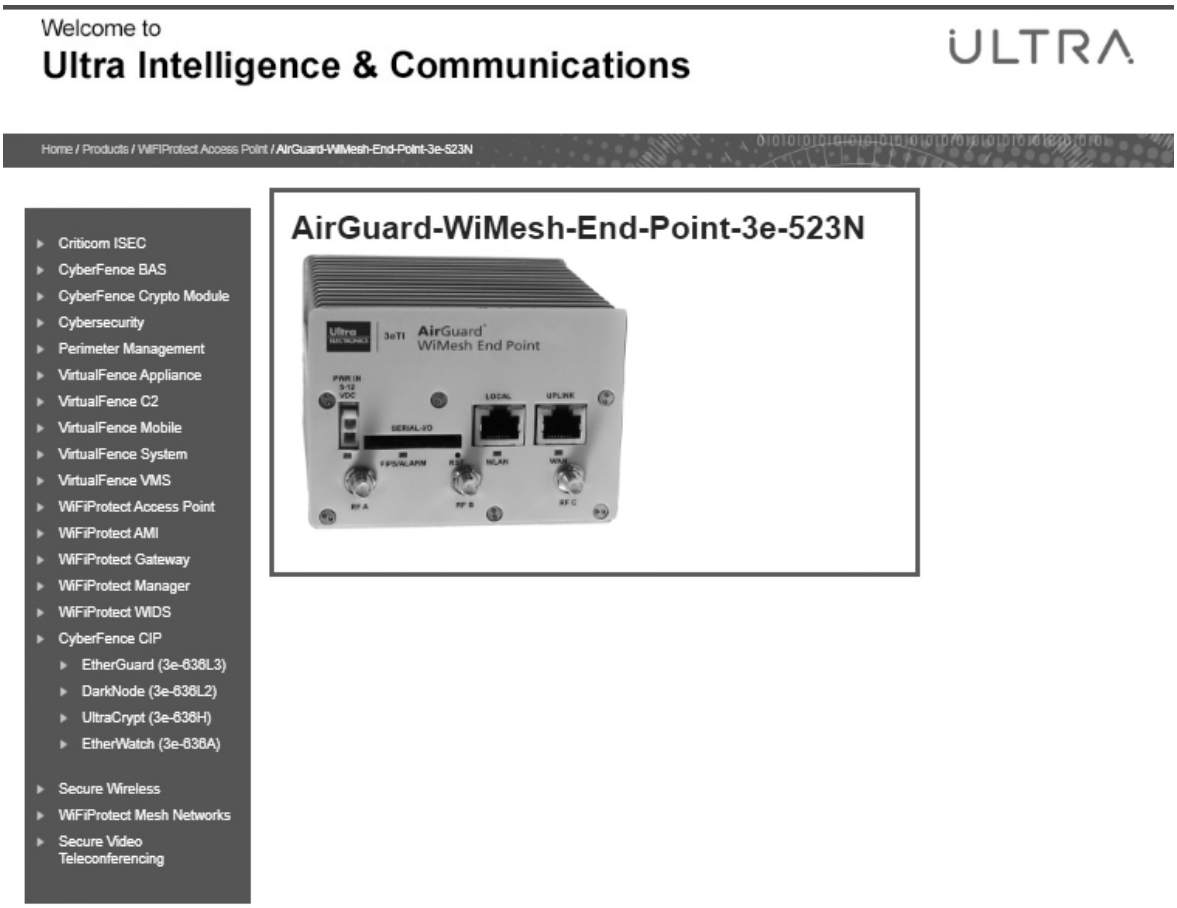
the "Accused Products"). The Accused Products and methods infringe at least claims 1, 2, 3, and 7 of the '405 Patent.

17. Claim 1 of the '405 Patent recites:

> 1. A method for setting up a connection for a communication network having a multiplicity of network nodes networked via links, comprising:
>
> (a) determining routes to destination network nodes of connection destinations for the network nodes;
>
> (b) allocating, in the network nodes, an allocation rule based on the determined routes, wherein, based on the allocation rule, a forwarding information item is allocated to a link leading to the destination network node and to a new forwarding information item for each destination network node; and
>
> (c) transmitting a setup message from an originating network node to one of the destination network nodes to prepare a subsequent transmission of data, such that a forwarding information item included in the setup message is to be read out, and
>
> (d) using the allocation rule, forwarding the setup message via a link allocated to the forwarding information item in the network node, after replacement of the forwarding information item in the setup message by the new forwarding information item allocated to the former forwarding information item.

18. Defendant infringes exemplar claim 1, as a non-limiting example only, by the Accused Products because:

a. The Accused Products practice a method for setting up a connection for a communication network (e.g., Wi-Fi) having a multiplicity of network nodes (e.g., the accused product) networked via links.



https://www.ultra-3eti.com/products/wifiprotect-access-point/airguard-wimesh-end-point-3e-523n/

As shown below, the accused products form a mesh network (i.e., communication network) via Wi-Fi links. It utilizes IEEE 802.11s standard to provide wireless mesh network functionality.

AirGuard WiMesh End Point
3e-523N

Certified secure 802.11n wireless data connectivity for critical network communications

3eTI's AirGuard® End Point is a next-generation secure wireless mesh device that provides connectivity for seamless voice, video and data communications in the most challenging environments. The freedom from geographical constraints makes the portable device ideal for military or defense environments such as operating facilities, base camps and field units. All of these require highly secure communications but do not readily accommodate trenching for wired solutions.

Using the latest 802.11n wireless technologies to achieve link rates of up to 300 Mbps, the AirGuard End Point is a self-forming, self-healing wireless mesh solution that meets the growing demand for streaming media and advanced applications. Devices, sensors or computers connected to the AirGuard End Point can communicate seamlessly over radio links secured by government-certified, field-proven encryption technologies. The WiMesh End Point supports two mesh options: 802.11s mesh and RSTP mesh. While RSTP mesh utilized lower bandwidth overhead, 802.11s offers better stability under more complex mesh-topology and interference conditions.

https://www.ultra-3eti.com/wp-content/uploads/2016/12/DS-AirGuard-WiMesh-End-Point-3e-523N.pdf

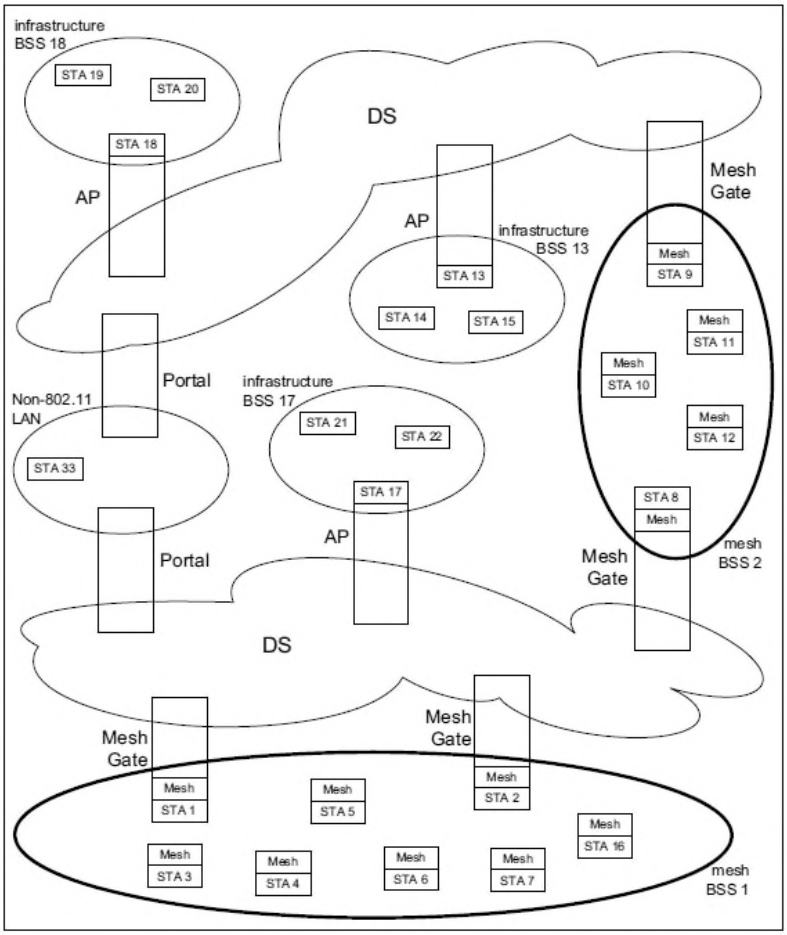
5.2.14.1 General

The IEEE 802.11 mesh facility provides MAC enhancements to support wireless LAN mesh topologies. The mesh facilities are available to mesh STAs that belong to a mesh BSS (MBSS). For a mesh STA that has not become a member of an MBSS, only the mesh discovery service is available. The enhancements that distinguish mesh STAs from non-mesh STAs are collectively termed the "mesh facility". The mesh-specific mechanisms vary among implementations.

5.2.14.2 Overview of the mesh BSS

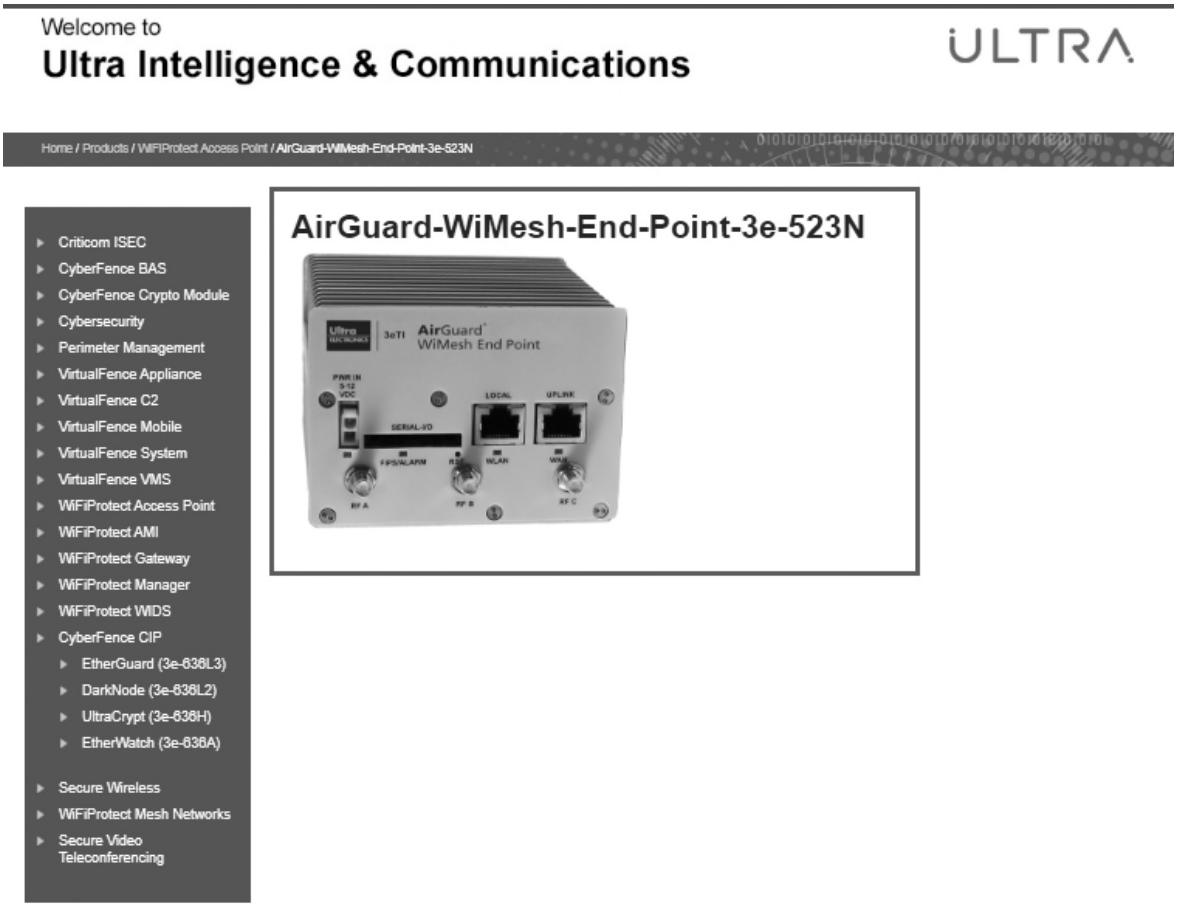
A mesh BSS is an IEEE 802.11 LAN consisting of autonomous STAs. Inside the mesh BSS, all STAs establish peer-to-peer wireless links and transfer messages mutually. Further, using the multi-hop capability, messages can be transferred between STAs that are not in direct communication with each other over a single instance of the wireless medium. From the data delivery point of view, it appears as if all STAs in a mesh BSS are directly connected at the MAC layer even if the STAs are not within range of each other. The multi-hop capability enhances the range of the STAs and benefits wireless LAN deployments.

https://standards.ieee.org/standard/802_11s-2011.html



https://standards.ieee.org/standard/802_11s-2011.html

b. The Accused Products practice determining routes to destination network nodes of connection destinations for the network nodes. For example, , the Accused Product follow IEEE 802.11s standard. According to the standard, each device scans the communication network to find peer devices and establishes mesh peering. Each device finds route to the next destination for transmission of packets in the multi-hop mesh network. The Accused Products thus determine routes to next destination device.



https://www.ultra-3eti.com/products/wifiprotect-access-point/airguard-wimesh-end-point-3e-523n/

AirGuard WiMesh End Point
3e-523N

Certified secure 802.11n wireless data connectivity for critical network communications

3eTI's AirGuard® End Point is a next-generation secure wireless mesh device that provides connectivity for seamless voice, video and data communications in the most challenging environments. The freedom from geographical constraints makes the portable device ideal for military or defense environments such as operating facilities, base camps and field units. All of these require highly secure communications but do not readily accommodate trenching for wired solutions.

Using the latest 802.11n wireless technologies to achieve link rates of up to 300 Mbps, the AirGuard End Point is a self-forming, self-healing wireless mesh solution that meets the growing demand for streaming media and advanced applications. Devices, sensors or computers connected to the AirGuard End Point can communicate seamlessly over radio links secured by government-certified, field-proven encryption technologies. The WiMesh End Point supports two mesh options: 802.11s mesh and RSTP mesh. While RSTP mesh utilized lower bandwidth overhead, 802.11s offers better stability under more complex mesh-topology and interference conditions.

https://www.ultra-3eti.com/wp-content/uploads/2016/12/DS-AirGuard-WiMesh-End-Point-3e-523N.pdf

As shown below, the accused product follows IEEE 802.11s standard. According to the standard, each device scans the communication network to find peer devices and establishes mesh peering. Each device finds route to the next destination for transmission of packets in the multi-hop mesh network. The accused product determines routes to next destination device.

11C.2.6 Scanning mesh BSSs

A mesh STA shall perform active scanning or passive scanning, depending on the value of the ScanMode parameter of the MLME-SCAN.request primitive (see 11.1.3), to discover neighbor mesh STAs. Upon receipt of an MLME-SCAN.request primitive with the Mesh ID parameter set to the wildcard Mesh ID, the STA shall passively scan for any Beacon frames, or actively transmit Probe Request frames containing the wildcard Mesh ID, as appropriate, depending on the value of ScanMode. Upon completion of scanning, an MLME-SCAN.confirm primitive is issued by the MLME indicating all of the discovery information received. Further, mesh STAs shall conform to the passive scan procedure as described in 11.1.3.1 and the active scan procedure as described in 11.1.3.2.

11C.2.7 Candidate peer mesh STA

When a mesh STA discovers a neighbor mesh STA through the scanning process and the discovered mesh STA is considered a candidate peer mesh STA, it may become a member of the mesh BSS of which the discovered mesh STA is a member and establish a mesh peering with the neighbor mesh STA.

The discovered neighbor mesh STA shall be considered a candidate peer mesh STA if and only if all of the following conditions are met:

a) The mesh STA uses the same mesh profile as the received Beacon or Probe Response frame indicates for the neighbor mesh STA.

NOTE—If the scanning mesh STA has not become a member of any MBSS yet, it might simply activate the same mesh profile as the discovered neighbor mesh STA's profile to fulfill this condition.

b) The Accepting Additional Mesh Peerings subfield in the Mesh Capability field in the received Beacon or Probe Response frame equals 1.

c) The mesh STA supports the data rates indicated by the BSSBasicRateSet of the received Beacon or Probe Response frame.

d) If both the scanning mesh STA and the discovered neighbor STA are HT STAs, the mesh STA uses the same BSSBasicMCSSet as the received Beacon or Probe Response frame indicates for the neighbor mesh STA.

e) If the scanning mesh STA has dot11MeshSecurityActivated set to true and the dot11MeshActiveAuthenticationProtocol is ieee8021x (2), either the scanning mesh STA has an active connection to an AS or the discovered mesh STA has the Connected to AS subfield in the Mesh Formation field in the Mesh Configuration element equal to 1 in the received Beacon or Probe Response frame.

https://standards.ieee.org/standard/802_11s-2011.html

11C.2.9 Establishing mesh peerings

Mesh peerings shall be established only with candidate mesh STAs that are members of the same MBSS.

A mesh peering is established between the mesh STA and the candidate peer mesh STA after the successful completion of the mesh peering management (MPM) protocol (see 11C.3) or of the authenticated mesh peering exchange (AMPE) (see 11C.5). When establishing a secure mesh peering, mesh STAs authenticate each other and create a mesh PMKSA before processing the AMPE (see 11C.3.3).

A candidate peer mesh STA becomes a peer mesh STA when a mesh peering is established between the two mesh STAs.

https://standards.ieee.org/standard/802_11s-2011.html

c. The Accused Products practice allocating, in the network nodes, an allocation rule (e.g., active path selection protocol) based on the determined

routes, wherein, based on the allocation rule, a forwarding information item is allocated to a link leading to the destination network node and to a new forwarding information item for each destination network node. According to IEEE 802.11s standard, an active path selection protocol is followed to select the best route for data transmission to a destination node. A mesh configuration element which is used to advertise mesh services provides information about the protocol which is allocated or followed in the network.

7.3.2.98 Mesh Configuration element

7.3.2.98.1 General

The Mesh Configuration element shown in Figure 7-95o130 is used to advertise mesh services. It is contained in Beacon frames and Probe Response frames transmitted by mesh STAs, and is also contained in Mesh Peering Open and Mesh Peering Confirm frames.

Element ID	Length	Active Path Selection Protocol Identifier	Active Path Selection Metric Identifier	Congestion Control Mode Identifier	Synchronization Method Identifier	Authentication Protocol Identifier	Mesh Formation Info	Mesh Capability
Octets: 1	1	1	1	1	1	1	1	1

Figure 7-95o130—Mesh Configuration element format

7.3.2.98.2 Active Path Selection Protocol Identifier

The Active Path Selection Protocol Identifier field indicates the path selection protocol that is currently activated in the MBSS. Table 7-43bj1 provides path selection protocol identifier values defined by this standard.

Table 7-43bj1—Active Path Selection Protocol Identifier field values

Value	Meaning
0	Reserved

Table 7-43bj1—Active Path Selection Protocol Identifier field values *(continued)*

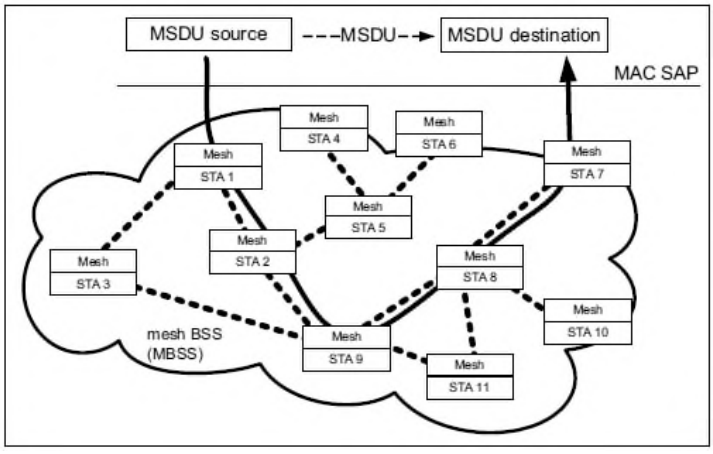
Value	Meaning
1	Hybrid wireless mesh protocol (default path selection protocol) defined in 11C.9 (default path selection protocol)
2–254	Reserved
255	Vendor specific (The active path selection protocol is specified in a Vendor Specific element)

5.2.14.5.9 Mesh path selection and forwarding

Mesh path selection enables path discovery over multiple instances of the wireless medium within a mesh BSS. The overview of the mesh path selection framework is described in 11C.7. The hybrid wireless mesh protocol (HWMP) is defined as the default path selection protocol for the mesh BSS. HWMP provides both proactive path selection and reactive path selection. The details of HWMP are described in 11C.9. The path selection protocol uses link metrics in the assessment of a mesh path to the destination. The airtime link metric is the default link metric. It is defined in 11C.8.

Once the mesh path of a particular pair of the source mesh STA and the destination mesh STA is found through the mesh path selection function, mesh STAs propagate the data by the forwarding function. The details of the forwarding function are described in 9.22.

As a result of the mesh path selection and forwarding, MSDUs are transmitted among all the mesh STAs in a mesh BSS, even if the mesh STAs are not neighbor STAs of each other. Figure 5-6d depicts the MSDU transfer within a mesh BSS.

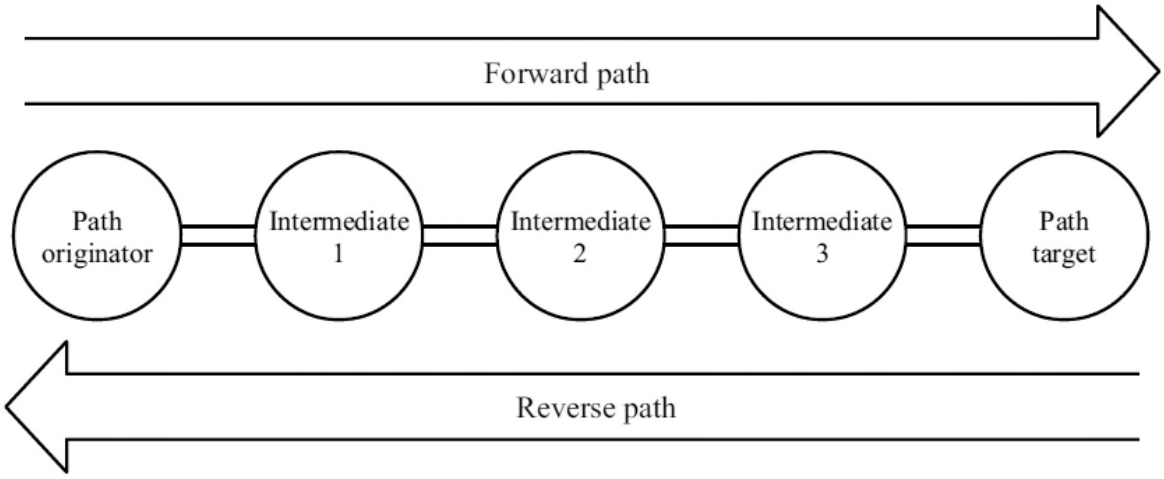


As shown below, while utilizing the active path selection protocol to determine the best path to a destination node, a hop which lies in route receives a path request PREQ with a forwarding information item, wherein basic forwarding information includes destination address, next-hop

address, precursor list and lifetime of the forwarding information item. If it determines it is not the destination it updates the forwarding information, the next-hop address, precursor list and lifetime of the forwarding information item, and transmit to the next-hop.

This subclause describes terminology for HWMP, especially for the process of path discovery. Terms such as Path Originator or Path Target designate very specific entities within the path discovery process. They stay with the same assigned entity for the whole path discovery process and other procedures related to this path discovery. Figure 11C-4 illustrates an example utilizing this terminology.

NOTE—Both the path target and path originator are a path destination for the forward path and the reverse path respectively.



forwarding information: The forwarding information maintained by an originator mesh STA, an intermediate mesh STA, or a target mesh STA that allows the mesh STA to perform its path selection and forwarding functions.

The terminology used when discussing forwarding information is relative to the mesh STA (reference mesh STA, given mesh STA or local mesh STA) and a particular mesh destination of the path. The following terms are specific to a given instance of the forwarding information:

- **destination mesh STA:** The end station (mesh STA) of a (forward or reverse) path.
- **destination mesh STA address:** The MAC address of the destination mesh STA.
- **destination HWMP sequence number:** The HWMP sequence number of the destination mesh STA.
- **next-hop mesh STA:** The next-hop mesh STA is the next peer mesh STA on the mesh path to the destination mesh STA.
- **next-hop mesh STA address:** The MAC address of the next-hop mesh STA.

9.22.2 Forwarding information

Forwarding information is created by the active mesh path selection protocol and is utilized for MSDU/ MMPDU forwarding as described in 9.22.4 and 9.22.6.2.

The basic forwarding information to a destination mesh STA consists of the destination mesh STA address, the next-hop address, the precursor list, and the lifetime of this forwarding information.

An entry in the precursor list contains the precursor mesh STA address and the lifetime of this entry. If an existing entry in a precursor list is updated, the lifetime is the maximum of the current and the updated value. If the lifetime of a precursor expires, it will be deleted from the precursor list. Precursors are used to identify legitimate transmitters of individually addressed frames (see 9.22.4.2) and for the notification of link failures (in case of HWMP, see 11C.9.11).

The forwarding information shall be considered as invalid if its lifetime has expired. Also, forwarding information is marked as invalid when certain conditions are met in the processing of mesh path selection elements, e.g., path error processing in HWMP (11C.9.11.4).

The active path selection protocol may define additional parameters in the forwarding information. Details on the additional parameters of the forwarding information constructed by the hybrid wireless mesh protocol (HWMP) are described in 11C.9.8.4.

11C.9.3 On-demand path selection mode

If a source mesh STA needs to find a path to a destination mesh STA using the on-demand path selection mode, it broadcasts a PREQ with the path target specified in the list of targets and the metric field initialized to the initial value of the active path selection metric.

When a mesh STA receives a new PREQ, it creates or updates its path information to the originator mesh STA and propagates the PREQ to its neighbor peer mesh STAs if the PREQ contains a greater HWMP sequence number, or the HWMP sequence number is the same as the current path and the PREQ offers a

better metric than the current path. Each mesh STA may receive multiple copies of the same PREQ that originated at the originator mesh STA, each PREQ traversing a unique path.

Whenever a mesh STA propagates a PREQ, the metric field in the PREQ is updated to reflect the cumulative metric of the path to the originator mesh STA. After creating or updating a path to the originator mesh STA, the target mesh STA sends an individually addressed PREP back to the originator mesh STA.

If the mesh STA that received a PREQ is the target mesh STA, it sends an individually addressed PREP back to the originator mesh STA after creating or updating a path to the originator mesh STA.

The PREQ provides the TO (Target Only) subfield that allows path selection to take advantage of existing paths to the target mesh STA by allowing an intermediate mesh STA to return a PREP to the originator mesh STA. If the TO (Target Only) subfield is 1, only the target mesh STA responds with a PREP. The effect of setting the TO (Target Only) subfield to 0 is the quick establishment of a path using the PREP generated by an intermediate mesh STA, allowing the forwarding of MSDUs with a low path selection delay. In order to select (or validate) the best path during the path selection procedure, the intermediate mesh STA that responded with a PREP propagates the PREQ with the TO (Target Only) subfield set to 1. This prevents all other intermediate mesh STAs on the way to the target from sending a PREP.

Intermediate mesh STAs create a path to the target mesh STA on receiving the PREP, and also forward the PREP toward the originator. When the originator receives the PREP, it creates a path to the target mesh STA. If the target mesh STA receives further PREQs with a better metric, then the target updates its path to the originator with the new path and also sends a new PREP to the originator along the updated path. A bidirectional, best metric end-to-end path is established between the originator and target mesh STA.

https://standards.ieee.org/standard/802_11s-2011.html

d. The Accused Products practice transmitting a setup message (e.g., a mesh data frame) from an originating network (e.g., the accused product) node to one of the destination network nodes (e.g., the product to which frame is transmitted from the accused product) to prepare a subsequent transmission of data, such that a forwarding information item included in the setup message is to be read out. According to the standard, a source node transmits a mesh data frame to a destination node via the best path determined by the active path selection protocol. The source node transmits the mesh data frame including forwarding information item, wherein basic forwarding information includes destination address, next-hop address, precursor list and lifetime of the forwarding information. A hop which lies

in the determined best path, deciphers the frame and checks whether the frame is form peer address, destined for it and next-hop or destination node is reachable or not.

9.32.4.1 At source mesh STAs (individually addressed)

MSDUs sent by a mesh STA (as a consequence of an MA-UNITDATA.request with an individual destination address) and destined to another mesh STA in the MBSS shall be transmitted using a frame with the four-address MAC header format (with the Address Extension Mode subfield in the Mesh Control field set to 00 (binary)), where the four address fields are set as follows (see row "Mesh Data (individually addressed)" in

9.22.4 Addressing and forwarding of individually addressed Mesh Data frames

9.22.4.1 At source mesh STAs (individually addressed)

MSDUs sent by a mesh STA (as a consequence of an MA-UNITDATA.request with an individual destination address) and destined to another mesh STA in the MBSS shall be transmitted using a frame with the four-address MAC header format [with the Address Extension Mode subfield in the Mesh Control field set to 00 (binary)], where the four address fields are set as follows [see row "Mesh Data (individually addressed)" in Table 9-13]:

— Address 1: The address of the next-hop mesh STA (toward the destination mesh STA according to the forwarding information—see 9.22.2)

— Address 2: The address of the transmitter mesh STA

— Address 3: The address of the destination mesh STA

— Address 4: The address of the source mesh STA

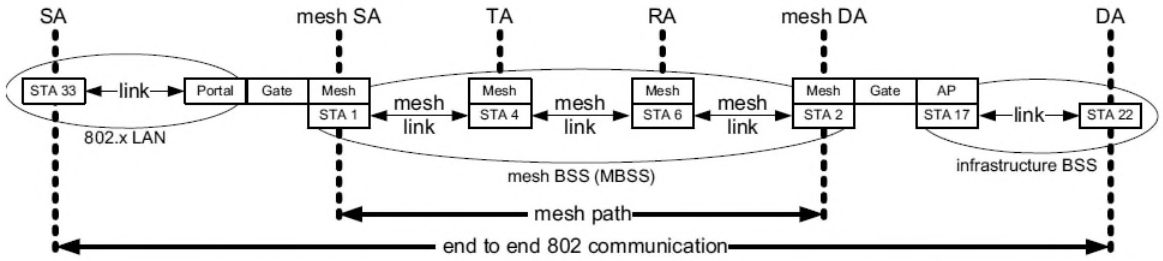


Figure 9-38—Example addressing for a Mesh Data frame

https://standards.ieee.org/standard/802_11s-2011.html

e. The Accused Products practice using the allocation rule, forwarding the setup message (e.g., a mesh data frame) via a link allocated to the forwarding information item in the network node, after replacement of the forwarding information item in the setup message by the new forwarding information item allocated to the former forwarding information item. According to the standard, an active path selection protocol is followed to determine the best path to a destination node. A source node transmits a mesh data frame to the destination node via the determined best path. A hop which lies in the path receives the frame and checks whether frame is destined for it, determining it is not the destination, it updates forwarding information, i.e., next-hop address, precursor list and lifetime of the forwarding information, and forwards the frame to the next node.

9.32.4.1 At source mesh STAs (individually addressed)

MSDUs sent by a mesh STA (as a consequence of an MA-UNITDATA.request with an individual destination address) and destined to another mesh STA in the MBSS shall be transmitted using a frame with the four-address MAC header format (with the Address Extension Mode subfield in the Mesh Control field set to 00 (binary)), where the four address fields are set as follows (see row "Mesh Data (individually addressed)" in

9.22.4 Addressing and forwarding of individually addressed Mesh Data frames

9.22.4.1 At source mesh STAs (individually addressed)

MSDUs sent by a mesh STA (as a consequence of an MA-UNITDATA.request with an individual destination address) and destined to another mesh STA in the MBSS shall be transmitted using a frame with the four-address MAC header format [with the Address Extension Mode subfield in the Mesh Control field set to 00 (binary)], where the four address fields are set as follows [see row "Mesh Data (individually addressed)" in Table 9-13]:

— Address 1: The address of the next-hop mesh STA (toward the destination mesh STA according to the forwarding information—see 9.22.2)

— Address 2: The address of the transmitter mesh STA

— Address 3: The address of the destination mesh STA

— Address 4: The address of the source mesh STA

NOTE 2—The forwarding of individually addressed Mesh Data frames uses only mesh STA addresses in fields Address 1, Address 2, Address 3, and Address 4. This allows intermediate mesh STAs to forward Mesh Data frames without necessarily having any knowledge of the addresses of the source and destination end stations, which might be external addresses. Thus, proxy information only needs to be maintained by proxy mesh gates and by source mesh STAs.

The term *source mesh STA* refers to the first mesh STA on a mesh path. A source mesh STA may be a mesh STA that is the initial source of an MSDU/MMPDU or a mesh STA that receives an MSDU/MMPDU from a mesh path or from a STA outside the mesh BSS and translates and forwards the MSDU/MMPDU on the mesh path. The address of the source mesh STA is referred to as the Mesh SA.

The term destination mesh STA refers to the final mesh STA on a mesh path. A destination mesh STA may be a mesh STA that is the final destination of an MSDU/MMPDU or a mesh STA that receives an MSDU/MMPDU from a mesh path and translates and forwards the MSDU/MMPDU on another mesh path or to a STA outside of the mesh BSS. The address of the destination mesh STA is referred to as the Mesh DA.

In group addressed Mesh Data frames, Address 1 and Address 2 correspond to the group address and the mesh STA transmitter address (TA). Address 3 corresponds to the mesh source address (mesh SA) of the group addressed Mesh Data frame. The Address Extension Mode indicates the presence of an optional address extension field Address 4 in the Mesh Control field that corresponds to the source address (SA) of external STAs that communicate over the mesh BSS via proxy mesh gates.

If Address 3 does not match the mesh STA's own address, but is a known individual destination MAC address in the forwarding information then the following actions are taken:

- The lifetime of the forwarding information to the destination (Address 3) is set to its initial value.
- The lifetime of the forwarding information to the source (Address 4) is set to its initial value.
- The lifetime of the precursor list entry for the precursor to the destination (Address 2) is set to the maximum of the initial value and the current value.
- The lifetime of the precursor list entry for the precursor to the source (next hop to the destination) is set to the maximum of the initial value and the current value.
- The Mesh TTL in the corresponding Mesh Control field of the collected MSDU is decremented by 1. If zero has been reached, the MSDU shall be discarded.
- If the MSDU has not been discarded, the mesh STA shall forward the MSDU via a frame with the Address 1 field set to the MAC address of the next-hop mesh STA as determined from the forwarding information (see 9.22.2) and the Address 2 field set to its own MAC address and queue the frame for transmission.

https://standards.ieee.org/standard/802_11s-2011.html

19. The foregoing structure, function, and operation of the exemplary Accused Products meet all limitations of at least exemplary claim 1 of the '405 Patent

20. Defendant infringes exemplary claim 2, as a non-limiting example only, by the Accused Products because:

a. The accused product practices the method of claim 1, wherein before the setup message (e.g., a mesh data frame) is transmitted; the allocation rule (e.g., active path selection protocol) is setup in the network nodes. According to the standard, an active path selection protocol is setup in the communication network before transmitting the setup message.

7.3.2.98 Mesh Configuration element

7.3.2.98.1 General

The Mesh Configuration element shown in Figure 7-95o130 is used to advertise mesh services. It is contained in Beacon frames and Probe Response frames transmitted by mesh STAs, and is also contained in Mesh Peering Open and Mesh Peering Confirm frames.

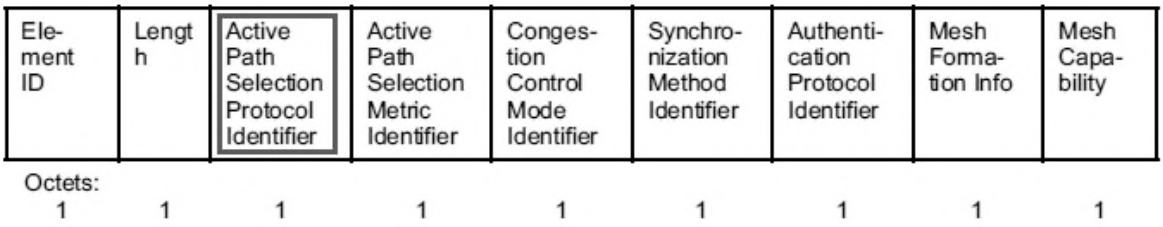


Figure 7-95o130—Mesh Configuration element format

7.3.2.98.2 Active Path Selection Protocol Identifier

The Active Path Selection Protocol Identifier field indicates the path selection protocol that is currently activated in the MBSS. Table 7-43bj1 provides path selection protocol identifier values defined by this standard.

Table 7-43bj1—Active Path Selection Protocol Identifier field values

Value	Meaning
0	Reserved

Table 7-43bj1—Active Path Selection Protocol Identifier field values *(continued)*

Value	Meaning
1	Hybrid wireless mesh protocol (default path selection protocol) defined in 11C.9 (default path selection protocol)
2–254	Reserved
255	Vendor specific (The active path selection protocol is specified in a Vendor Specific element)

https://standards.ieee.org/standard/802_11s-2011.html

21. Defendant infringes exemplary claim 3, as a non-limiting example only, by the Accused Products because:

a. The accused product practices the method of claim 1, wherein, in a network node receiving a setup message the forwarding information item included in the setup message is replaced by a new forwarding information item allocated to the forwarding information item in the network node, by means of which new information item the setup message is then forwarded. According to the standard, an active path selection protocol is followed to determine the best path to a destination node. A source node transmits a mesh data frame to the destination node via the determined best path. A hop which lies in the path receives the frame and checks whether frame is destined for it, determining it is not the destination, it updates forwarding information, i.e., next-hop address, precursor list and lifetime of the forwarding information, and forwards the frame to the next node.

9.32.4.1 At source mesh STAs (individually addressed)

MSDUs sent by a mesh STA (as a consequence of an MA-UNITDATA.request with an individual destination address) and destined to another mesh STA in the MBSS shall be transmitted using a frame with the four-address MAC header format (with the Address Extension Mode subfield in the Mesh Control field set to 00 (binary)), where the four address fields are set as follows (see row "Mesh Data (individually addressed)" in

5.2.2 MA-UNITDATA.request

5.2.2.1 Function

This primitive requests a transfer of an MSDU from a local LLC sublayer entity to a single peer LLC sublayer entity, or multiple peer LLC sublayer entities in the case of group addresses.

5.2.2.4 Effect of receipt

On receipt of this primitive, the MAC sublayer entity determines whether it is able to fulfill the request according to the requested parameters. A request that cannot be fulfilled according to the requested parameters is discarded, and this action is indicated to the LLC sublayer entity using an MA-UNITDATA-STATUS.indication primitive that describes why the MAC was unable to fulfill the request. If the request can be fulfilled according to the requested parameters, the MAC sublayer entity appends all MAC specified fields (including DA, SA, FCS, and all fields that are unique to IEEE Std 802.11), passes the properly formatted frame to the lower layers for transfer to a peer MAC sublayer entity or entities (see 5.1.4), and indicates this action to the LLC sublayer entity using an MA-UNITDATA-STATUS.indication primitive with transmission status set to Successful.

9.22.4 Addressing and forwarding of individually addressed Mesh Data frames

9.22.4.1 At source mesh STAs (individually addressed)

MSDUs sent by a mesh STA (as a consequence of an MA-UNITDATA.request with an individual destination address) and destined to another mesh STA in the MBSS shall be transmitted using a frame with the four-address MAC header format [with the Address Extension Mode subfield in the Mesh Control field set to 00 (binary)], where the four address fields are set as follows [see row "Mesh Data (individually addressed)" in Table 9-13]:

- Address 1: The address of the next-hop mesh STA (toward the destination mesh STA according to the forwarding information—see 9.22.2)
- Address 2: The address of the transmitter mesh STA
- Address 3: The address of the destination mesh STA
- Address 4: The address of the source mesh STA

https://standards.ieee.org/standard/802_11-2012.html

22. Defendant infringes exemplary claim 7, as a non-limiting example only, by the Accused Products because:

a. The Accused Products practice the method of Claim 1 such that in each case the new forwarding information item allocated to a forwarding information item in one of the network nodes is allocated, in the network node connected via the link also allocated and leading in the direction of the respective destination node, as forwarding information to a link leading in the direction of the same destination network node. According to the standard, an active

path selection protocol is followed to determine the best path to a destination node. A source node transmits a mesh data frame to the destination node via the determined best path. A hop which lies in the path receives the frame and checks whether frame is destined for it, determining it is not the destination, it updates forwarding information, i.e., next-hop address, precursor list and lifetime of the forwarding information, and forwards the frame to the next node. *See evidence above.*

23. Fairway has been damaged as a result of the infringing conduct by Defendant alleged above. Thus, Defendant is liable to Fairway in an amount that adequately compensates Fairway for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

24. Fairway and/or its predecessors-in-interest have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '200 Patent.

PRAYER FOR RELIEF

WHEREFORE, Fairway respectfully requests:

A. That Judgment be entered that Defendant has infringed at least one or more claims of the '405 Patent, directly and/or indirectly, literally and/or under the doctrine of equivalents;

B. An award of damages sufficient to compensate Fairway for Defendant's infringement under 35 U.S.C. § 284;

C. That the case be found exceptional under 35 U.S.C. § 285 and that Fairway be awarded its reasonable attorneys' fees;

D. Costs and expenses in this action;

E. An award of prejudgment and post-judgment interest; and

F. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Fairway respectfully demands a trial by jury on all issues triable by jury.

DATED October 31, 2020.

Respectfully submitted,

By: */s/ Neal Massand*
Neal Massand
Texas Bar No. 24039038
nmassand@nilawfirm.com

NI, WANG & MASSAND, PLLC
8140 Walnut Hill Ln., Ste. 500
Dallas, TX 75231
Tel: (972) 331-4600
Fax: (972) 314-0900

ATTORNEYS FOR PLAINTIFF FAIRWAY IP LLC